Direct Access

Es wird Zeit für eine neue Verbindung

Frank Carius

Net at Work
Building IT-Excellence.

Communication

Collaboration

Platform Services

Managed Service

Net at Work
Building IT-Excellence.

NoSpamProxy Protection

- Anti-Spam
- Anti-Virus

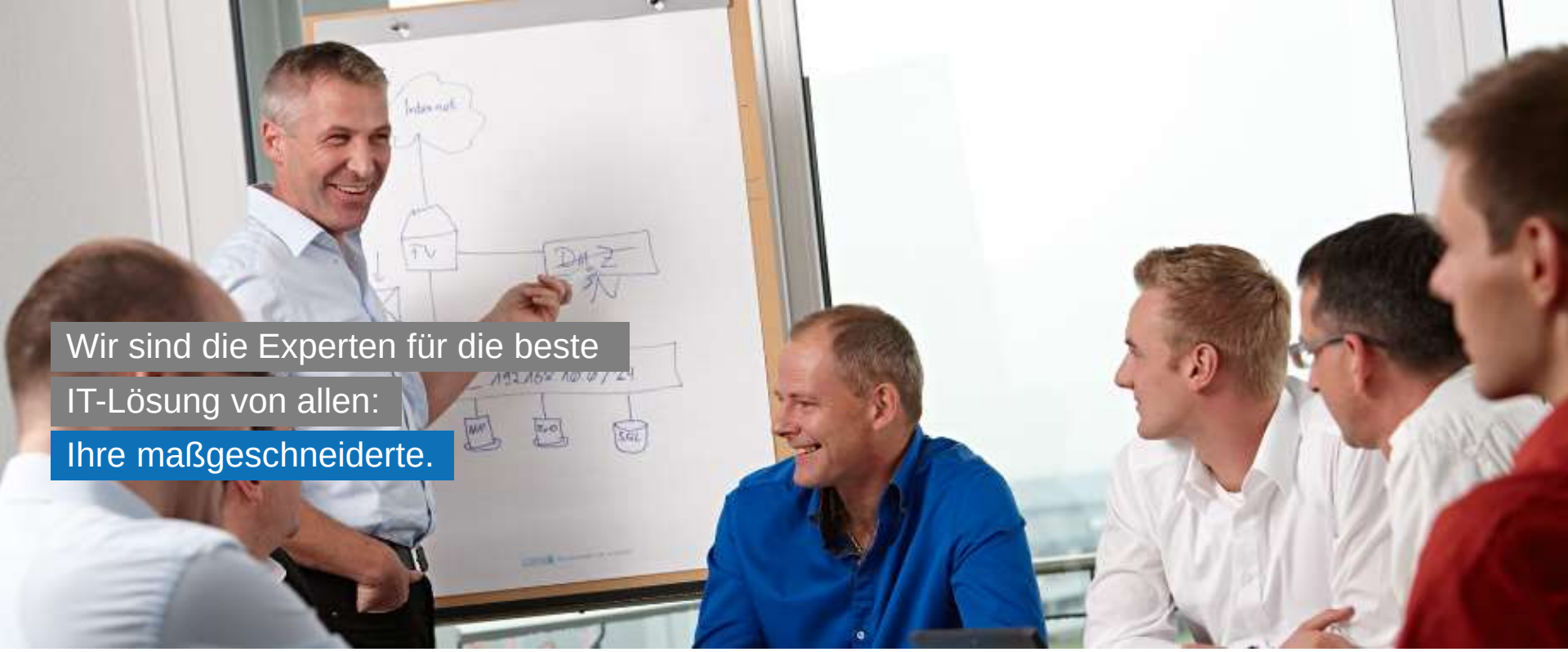
NoSpamProxy Encryption

- Verschlüsslung
- SMIME / PGP / PDFMail

NoSpamProxy Large Files

- Dateitransfer

Net at Work
Building IT-Excellence.



Standort Paderborn

Gründung 1995

40 Mitarbeiter

Microsoft Partner

Gold Messaging
Gold Communications
Gold Collaboration and Content
Gold Application Development

Net at Work

Building IT-Excellence.

Net at Work
Building IT-Excellence.

Direct Access

Gestern

Net at Work
Building IT-Excellence.

- VPN-Lösungen
  - Windows Routing und RAS
    - Verbindungsaufbau mühselig
    - PPTP ist unsicher
    - Firewall blockiert L2TP
  - 3rd Party VPN
    - Zusatzkosten
    - Zusätzliche Server
    - Getrenntes Management
    - Eigener Client muss verteilt werden
  - Browser-basiertes VPN
    - Gemischte Erfahrungen
- Betrieb (Windows VPN)
  - Benutzer „können“ kein VPN aufbauen
  - Manueller Verbindungsaufbau
  - Kein Management „von innen“

Brauchen wir noch ein VPN ?

Net at Work
Building IT-Excellence.

- Mobile Geräte über ActiveSync
- Outlook über Outlook AnyWhere
- RDP über Terminal Server Gateway
- OneDrive for Business
- Webzugriff für
  - Outlook WebApp
  - CRM
  - SharePoint
  - SCOM, PRTG, …
  - Exchange Control Panel
  - Lync Control Panel
  - Provisioning Systeme (z.B. Adaxes)

Aber …

Net at Work
Building IT-Excellence.

- Alles muss durch HTTPS
  - Andere Protokolle sind nicht „Firewall freundlich“
- Öffentliche Zertifikate
  - Da fremde Clients genutzt werden können
- Keine „integrierte“ Authentifizierung
  - Da kein Zugriff auf den KDC
- Outlook Anywhere/EWS
  - Kompletter Durchgriff auf fremden Geräten möglich
  - Keine „ActiveSync Policies“
  - Keine Quarantäne
- Nicht alle Dienste können „HTTPS“
- „Fremde“ Clients möglich
  - Keine Kontrolle
  - Keine Richtlinien
  - Keine Mindeststandards
  - Erschwerter Support

Direct Access Lösung

Net at Work
Building IT-Excellence.

- Bestandteil von Windows Server
  - Windows 2008R2 Server, UAG für IPv4 Support, zwei Public IP
  - Windows 2012RTM/R2, Single IP, Kein UAG
- Clients
  - Windows 7 Enterprise
  - Windows 8 Enterprise
  - Windows 8.1 Enterprise
- Konfiguration per Gruppenrichtlinie
  - Einfachste Konfiguration für den Administrator
  - Server und Clients müssen Domainmitglied sein
  - GPO für Clients UND Server
- Always-On VPN
  - Anwender bauen keine Verbindung auf/ab
  - Management „von Innen“
  - PC muss nur an sein, keine Benutzeranmeldung erforderlich
  - Keine Unterscheidung zwischen Intern und Extern
- IPv6 als Basis, HTTPS als Transport

Direct Access – Wichtige Fakten

Net at Work
Building IT-Excellence.

- Windows 2008R2/Windows 7 brauchen
  - IPv6 Deployment auf dem ersten Subnetz
  - DNS-Server mit IPv6-Adressen
  - Zwei aufeinanderfolgende öffentlicher IPv4-Adressen
  - PKI mit Zertifikaten und CRL
  - UAG für per IPv4 intern erreichbare Server
  - Gesonderter NLS-Server
- Windows 2012/Windows 8 machen es besser
  - NLS-Server kann auf DA-Server mitlaufen
  - Nur eine Public IPv4-Adresse
  - Keine PKI (außer mit Windows 7 Clients)
  - Kein IPv6 intern mehr erforderlich
  - Schnellerer Verbindungsaufbau
- Einschränkungen bleiben
  - IPv4-Only Hosts sind nur über „Namen“ erreichbar
  - Clientsoftware muss IPv6 unterstützen
  - Windows Enterprise Version als Desktop

Zusammenhänge

Routing

NAT

NAT64

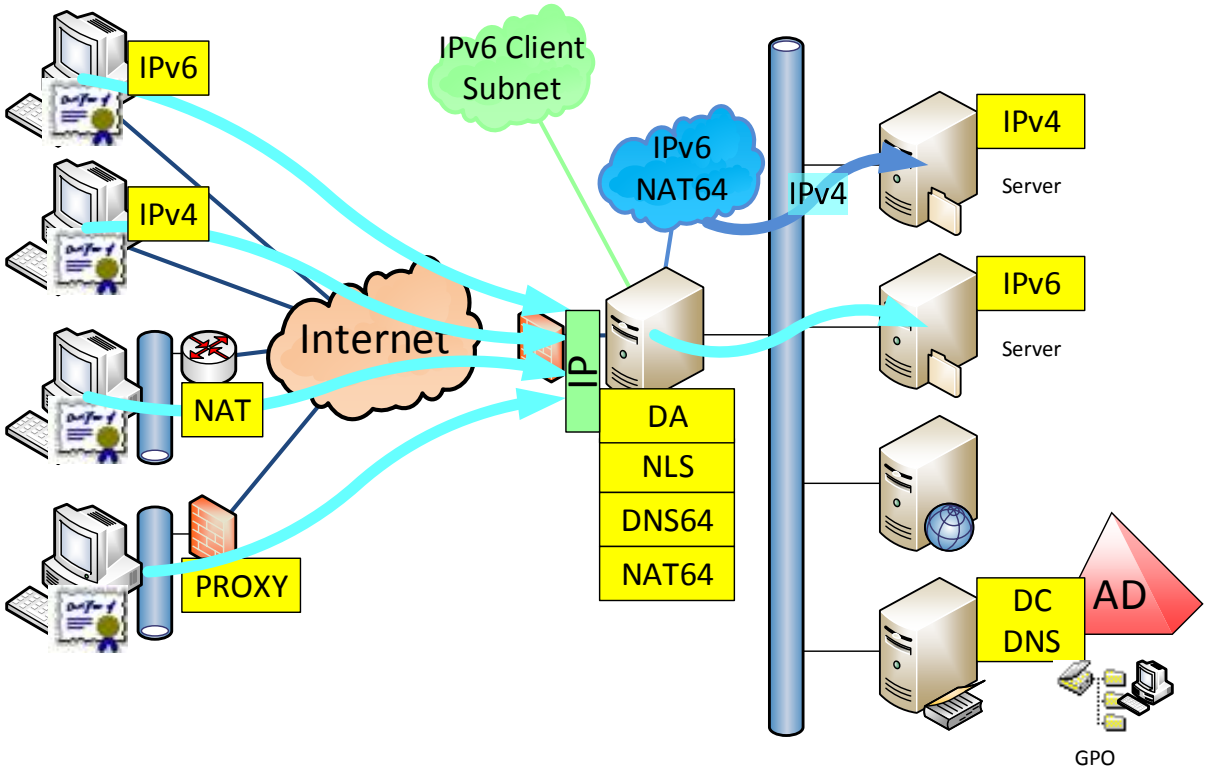
DNS

DNS64

IPHTTPS

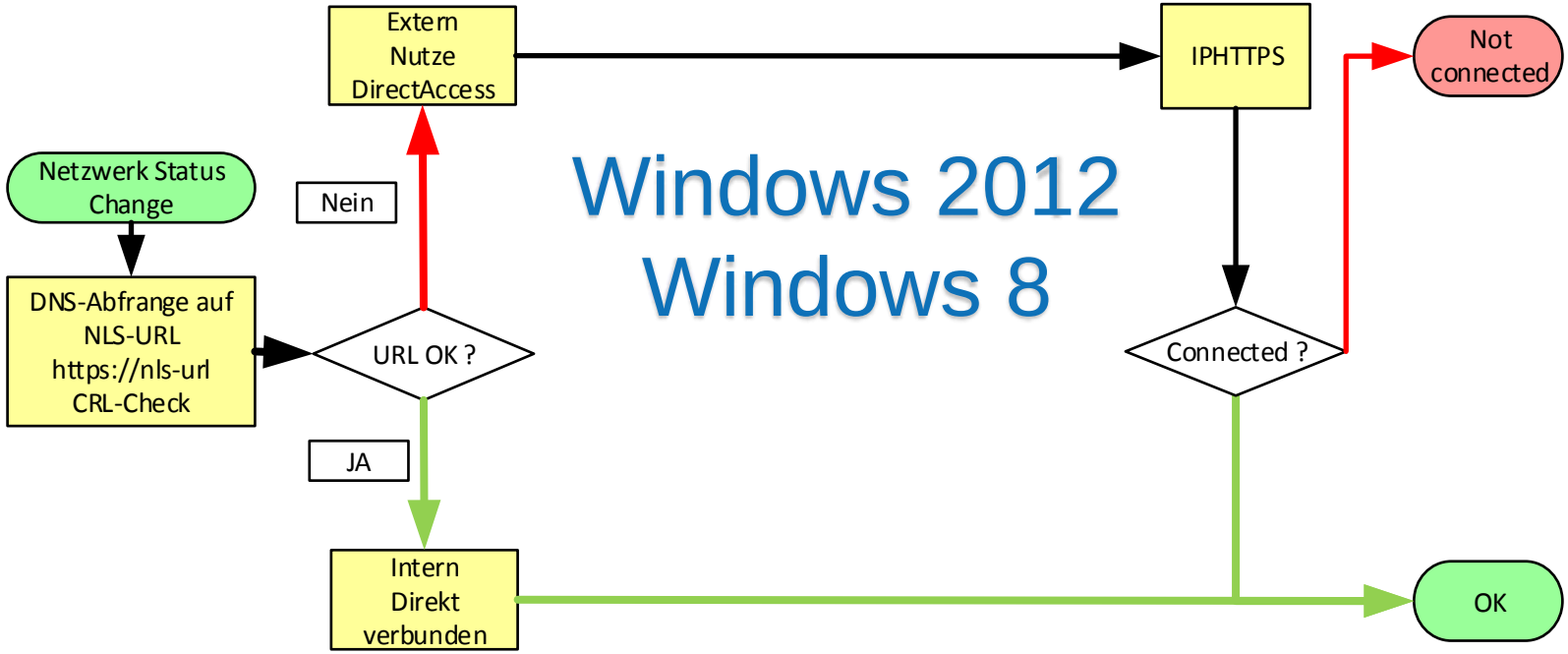
Basisnetzwerk

- Internes Netzwerk privaten IPv4
- Active Directory
- Gruppenrichtlinien
- DNS und DHCP
- Internet und Firewall



Network Location Service

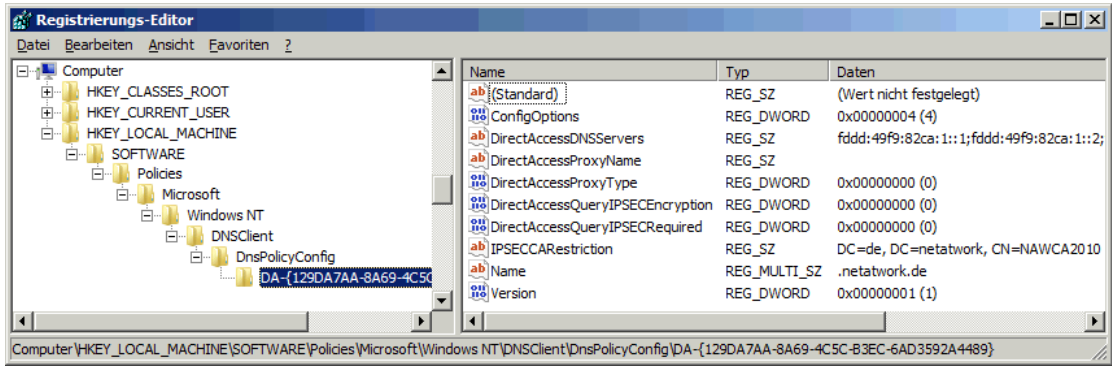
- Woher weiß der Client, ob er Intern oder Extern ist ?
- Client prüft den Network Location Service https://nls.server.fqdn – TLS Handshake muss passen
- NLS ist „mission critical“ !
- Client baut Verbindung auf



Wie wird der Client konfiguriert ?

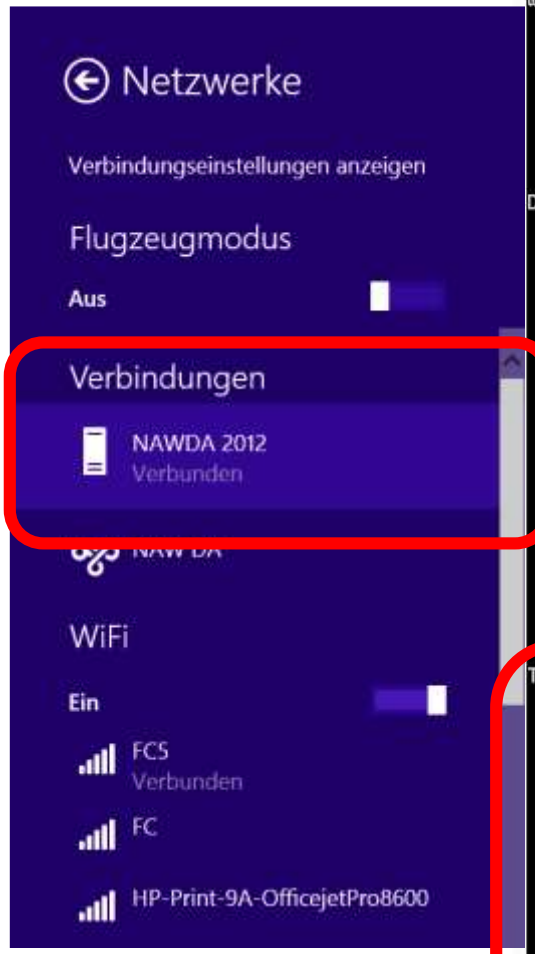
Net at Work
Building IT-Excellence.

- DA Assistent legt „Gruppenrichtlinien“ an
  - Enthalten den NLS-Server
  - Enthalten den DA-Server
  - Enthalten Zertifikatinformationen
  - Enthalten DNS-Informationen (Name Resolution Policy Table, NRPT)
- Client stellt Verbindung her
  - Prüft NLS-Service
  - Baut IPHTTP-Tunnel auf
  - Bekommt IPv6-Adresse aus dem Pool des Direct Access-Servers



IPConfig auf einem DA-Client

Net at Work
Building IT-Excellence.

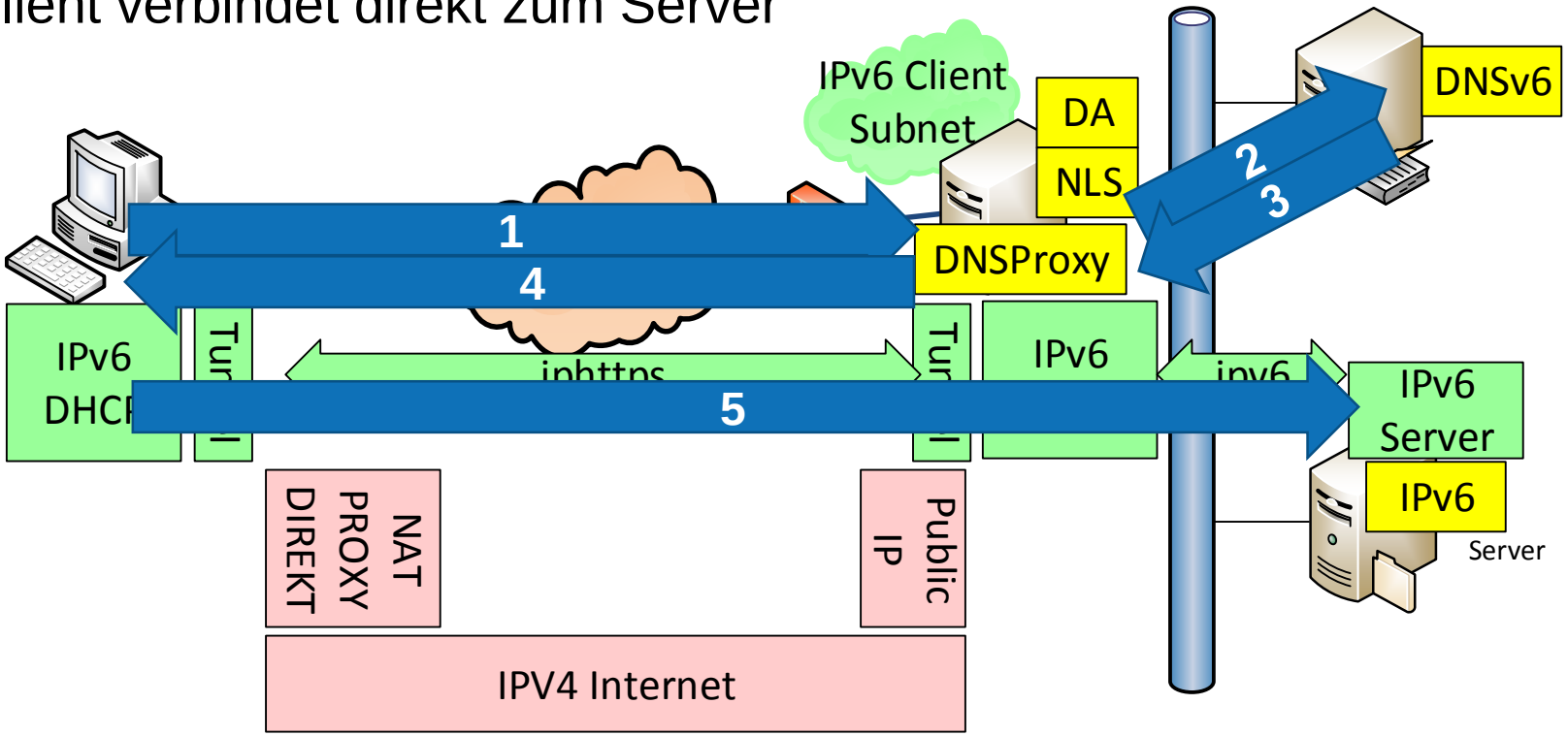


Eingabeaufforderung

```
C:\>ipconfig /all

Windows-IP-Konfiguration

   Hostname  . . . . . . . . . . . . : fcyoga
   Primäres DNS-Suffix . . . . . . . : netatwork.de
   Knotentyp . . . . . . . . . . . . : Hybrid
   IP-Routing aktiviert  . . . . . . : Nein
   WINS-Proxy aktiviert  . . . . . . : Nein
   DNS-Suffixsuchliste . . . . . . . : netatwork.de

Drahtlos-LAN-Adapter WiFi:

   Verbindungsspezifisches DNS-Suffix: fritz.box
   Beschreibung. . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7260
   Physische Adresse . . . . . . . . : F8-16-54-0A-00-F0
   DHCP aktiviert. . . . . . . . . . : Ja
   Autokonfiguration aktiviert . . . : Ja
   Verbindungslokale IPv6-Adresse  . : fe80::3826:4990:cfaf:22ae%3(Bevorzugt)
   IPv4-Adresse  . . . . . . . . . . : 192.168.178.55(Bevorzugt)
   Subnetzmaske  . . . . . . . . . . : 255.255.255.0
   Lease erhalten. . . . . . . . . . : Donnerstag, 26. März 2015 23:01:43
   Lease läuft ab. . . . . . . . . . : Sonntag, 5. April 2015 23:01:42
   Standardgateway . . . . . . . . . : 192.168.178.1
   DHCP-Server . . . . . . . . . . . : 192.168.178.1
   DHCPv6-IAID . . . . . . . . . . . : 66590292
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0
   DNS-Server  . . . . . . . . . . . : 192.168.178.1
   NetBIOS über TCP/IP . . . . . . . : Aktiviert

Tunneladapter iphttpsinterface:

   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : iphttpsinterface
   Physische Adresse . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2002:5042:141c:1000:a101:b18b:af84:c46a(Bevorzugt)
   Temporäre IPv6-Adresse. . . . . . : 2002:5042:141c:1000:5112:c13a:d1b:9647(Bevorzugt)
   Verbindungslokale IPv6-Adresse  . : fe80::a101:b18b:af84:c46a%19(Bevorzugt)
   Standardgateway . . . . . . . . . :
   DHCPv6-IAID . . . . . . . . . . . : 603979776
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0
   NetBIOS über TCP/IP . . . . . . . : Deaktiviert
```

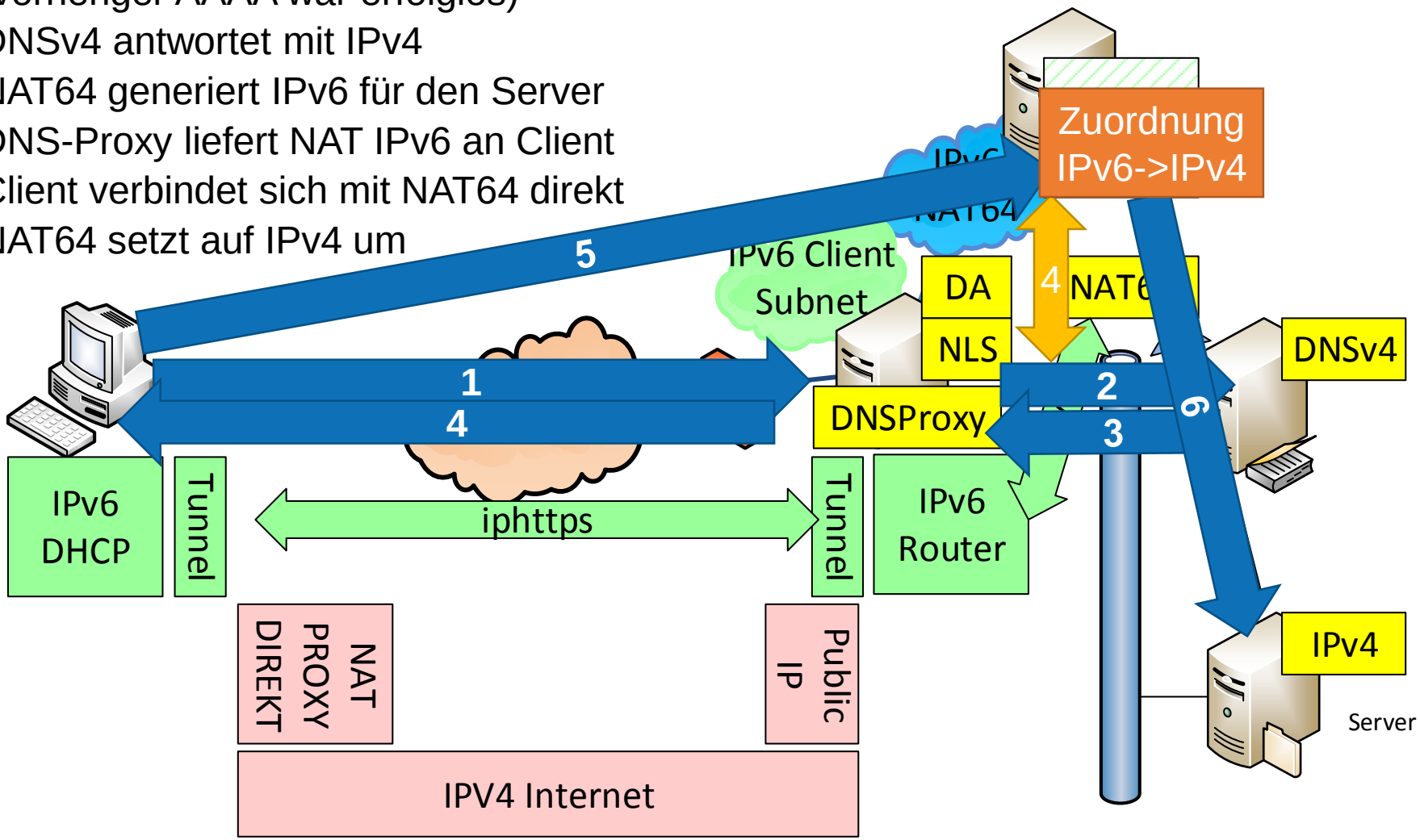
DNS und IP-Routing: IPv6 Server

- Client fragt den DNS-Proxy nach dem Namen
- DNS-Proxy stellt AAAA-Query an DNS
- DNSv6 antwortet mit IPv6
- DNSProxy liefert IPv6 an Client
- Client verbindet direkt zum Server



DNS und IP-Routing: IPv4 Server

- Client fragt den DNS-Proxy nach dem Namen
- DNS-Proxy stellt A-Query an DNS (vorheriger AAAA war erfolglos)
- DNSv4 antwortet mit IPv4
- NAT64 generiert IPv6 für den Server
- DNS-Proxy liefert NAT IPv6 an Client
- Client verbindet sich mit NAT64 direkt
- NAT64 setzt auf IPv4 um



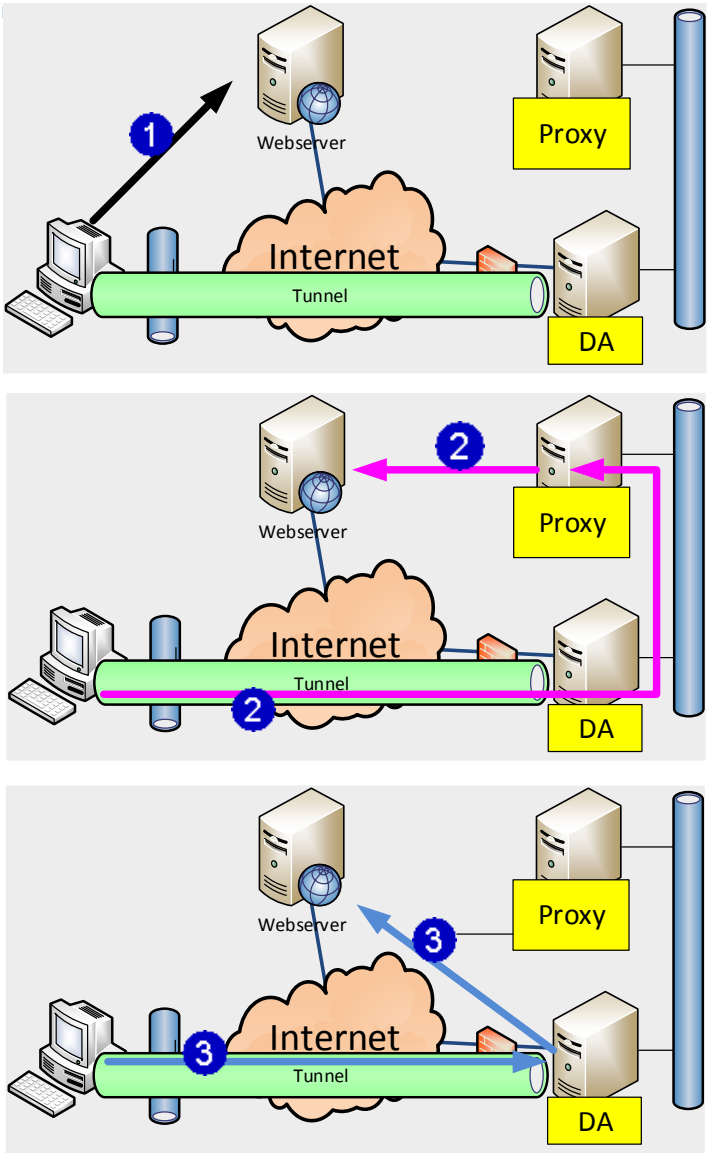
DNS64 und NAT64

Net at Work
Building IT-Excellence.

- Ein DA-Client kann NUR mit IPv6-Gegenstellen sprechen
- Ein DA-Client fragt immer den DNS-Proxy auf dem DA-Server
- Der DNS-Proxy fragt den internen DNS-Server
- DNS-Server liefert IPv6 oder IPv4-Adresse
  - IPv6-Antwort nur, wenn per IPv6 erreichbar
- IPv6-Server werden direkt angesprochen
  - intern ist IPv6 korrekt konfiguriert
  - Bitte kein ISATAP !!!
- IPv4-Server werden hinter einer IPv6 Adresse per Reverse-NAT versteckt
  - NAT64-Komponente setzt Pakete entsprechend um
- DA-Client kann nie IPv4-Adressen direkt ansprechen
  - Hosts müssen per DNS aufgelöst werden, um NAT64 zu aktivieren
- NAT64 ist erst seit Windows 2012 „eingebaut“
  - Mit Windows 2008R2 DA musste ein NAT64/DNS64 Service extra installiert werden, z.B. UAG

Internet Zugriff für DA Clients

- Bypass
  - Internet Traffic direkt zum Ziel
  - Kein Verkehr auf dem Tunnel
  - Auch für selektive Hosts und Domains
- Tunnel Mode mit HTTP-Proxy
  - Browser via HTTP-Proxy
  - Zentrale Steuerung/Filterung
  - Doppelter Verkehr am Firmen-Link
- Tunnel ohne Proxy
  - Source IP des Direct Access wird genutzt
  - Direct Access muss also „raus“ dürfen
- Lokaler Traffic
  - Zugriffe auf Dienste im lokalen Netz gehen immer, z.B. Drucker



Nachzügler

Net at Work
Building IT-Excellence.

- Management von Clients
  - Über Direct Access können Clients vom zentralen LAN verwaltet werden
  - Voraussetzung ist IPv6 !!!
  - Direct Access kann sogar für „Management Only“ eingesetzt werden
- Hochverfügbarkeit
  - DirectAccess ist HTTPS
  - Lastverteilung mit NLB oder externem Loadbalancer
  - Denken Sie an NLS Verfügbarkeit !!
- Geografische Steuerung
  - Mehrere DA-Server in verschiedenen Ländern möglich
  - Client nutzt immer den gleichen DA-Zugang
  - Steuerung per Gruppenrichtlinien und Computergruppen

Einrichtung und Konfiguration

Rollen

Features

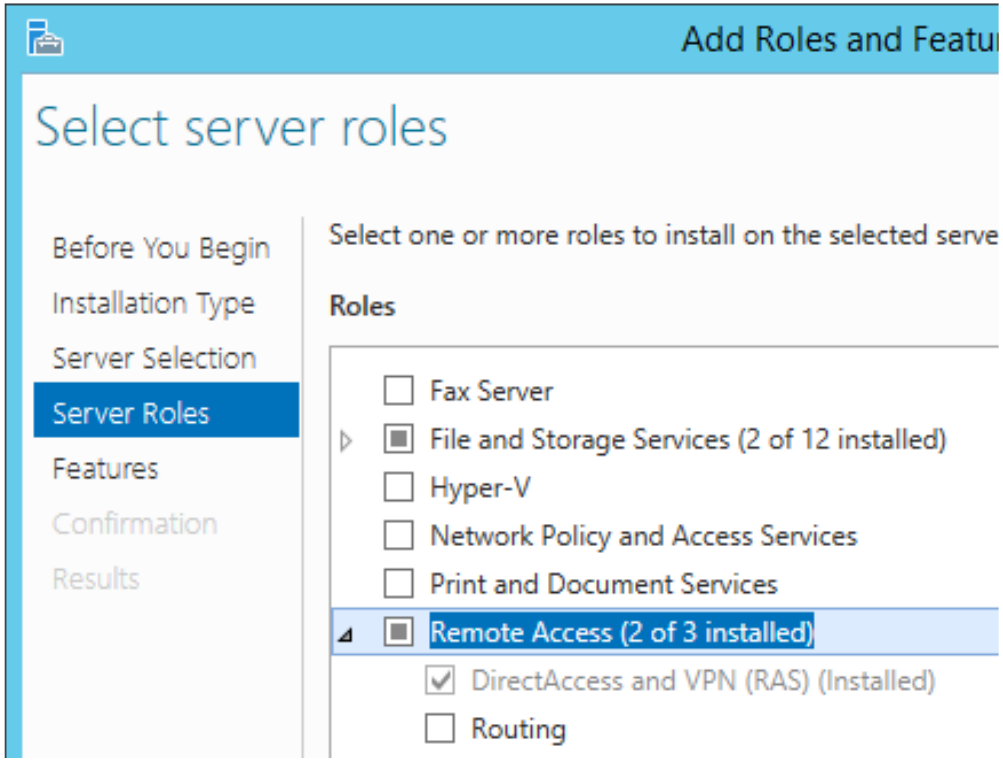
Adressen

Richtlinien

Schritte der Einrichtung

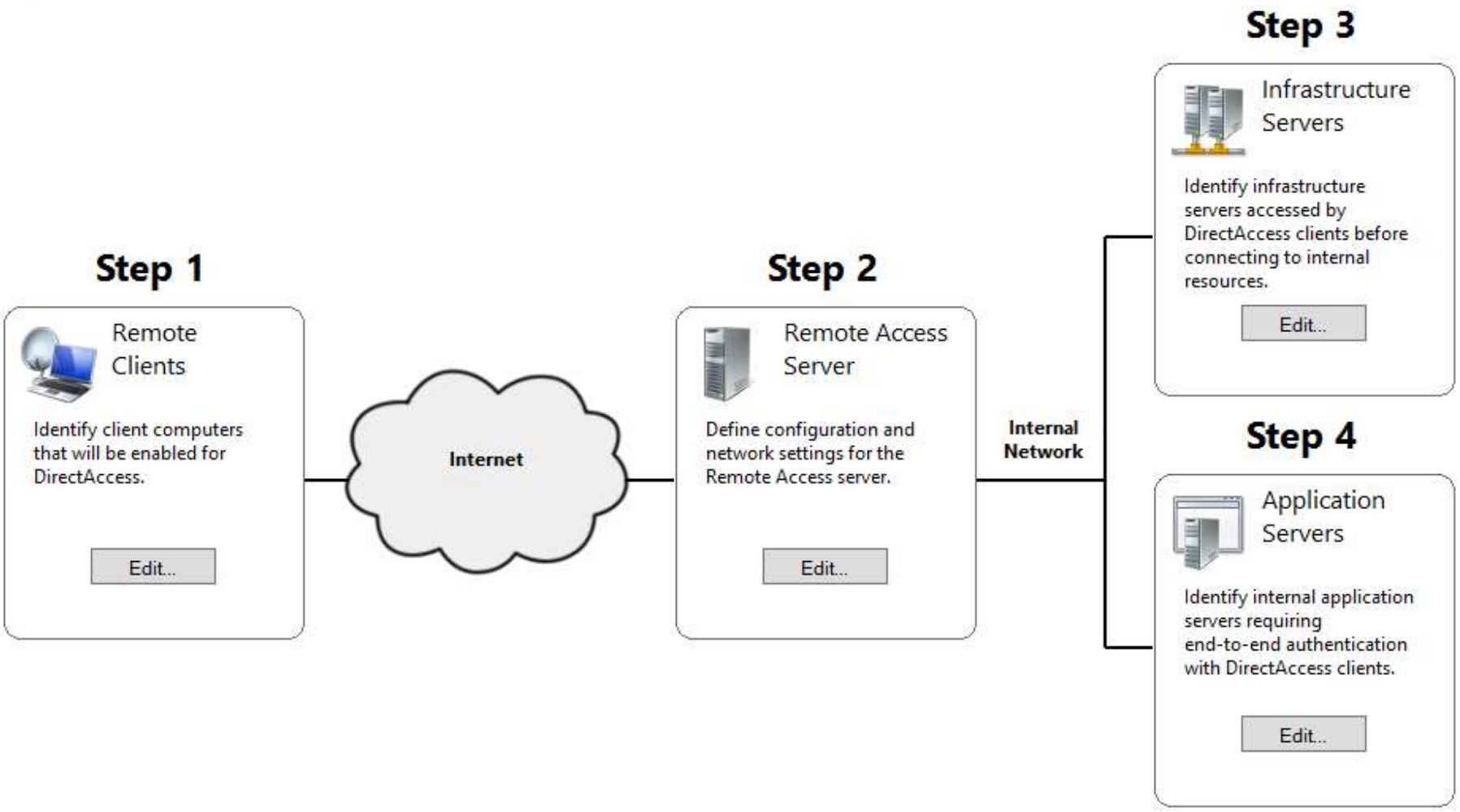
Net at Work
Building IT-Excellence.

- Basis schaffen
  - Windows 2012 R2 Server
  - 1x Netzwerk nach „draußen“
  - 1x Firewall 443 eingehend
  - 1x DNS-Eintrag extern
  - 1x DNS-Eintrag intern (Connectivity Check)
  - 1x Netzwerk nach „drinnen“
  - Mitglied der Domäne
- Add Roles & Features
  - Remote Access
  - Updates installieren
- Konfigurieren
- Testen
- Ausrollen



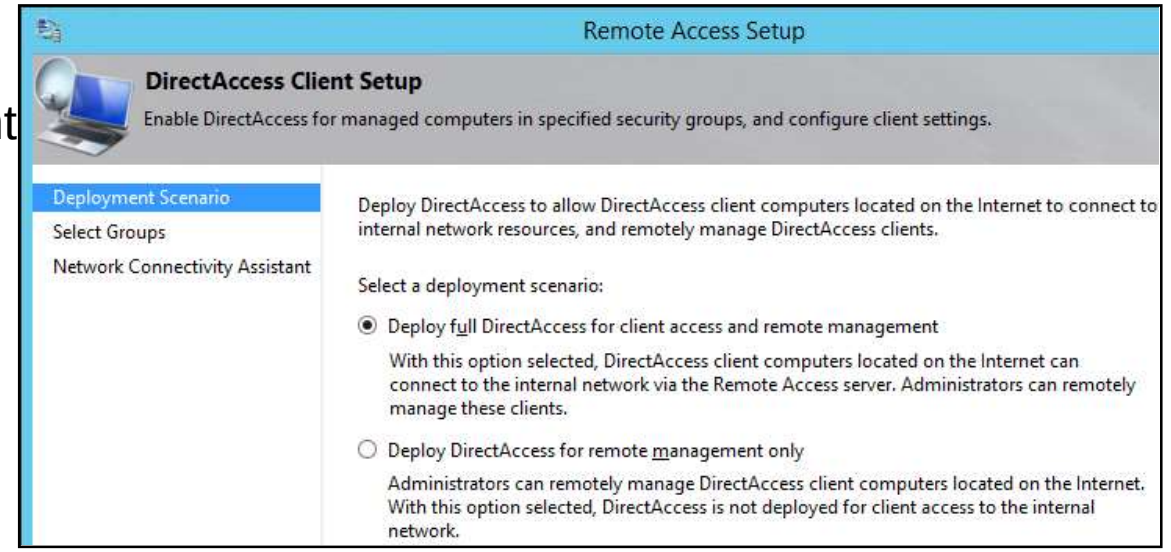
Konfiguration

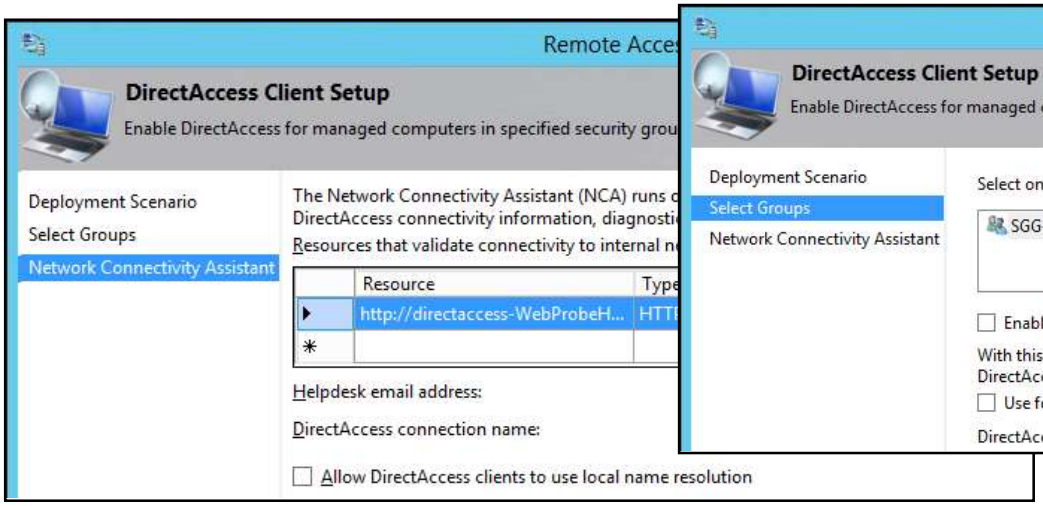
Net at Work
Building IT-Excellence.

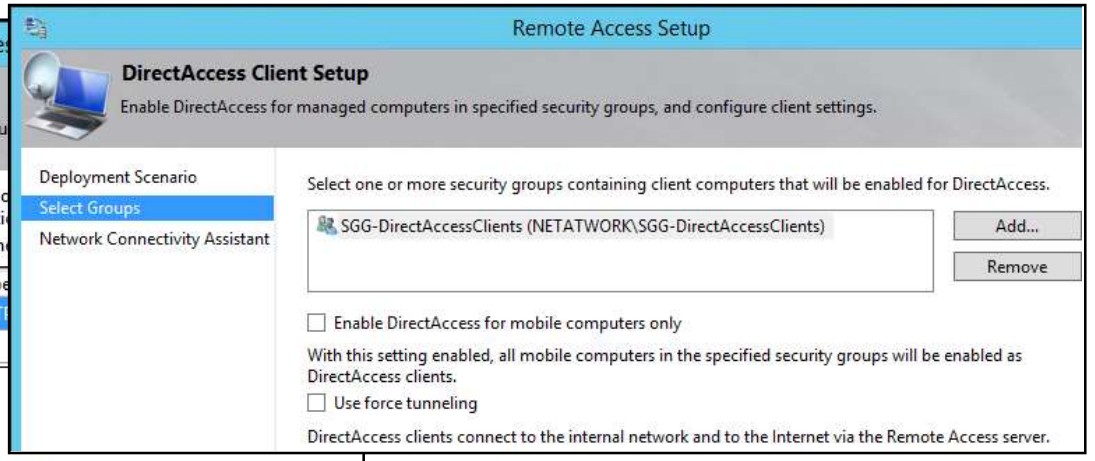


Schritt 1: Remote Client festlegen

- Deployment Szenario
  - Client und Management
  - Management only
- Zielclients
  - Windows Gruppen
- Connectivity Check
  - Mit „VPN Name“



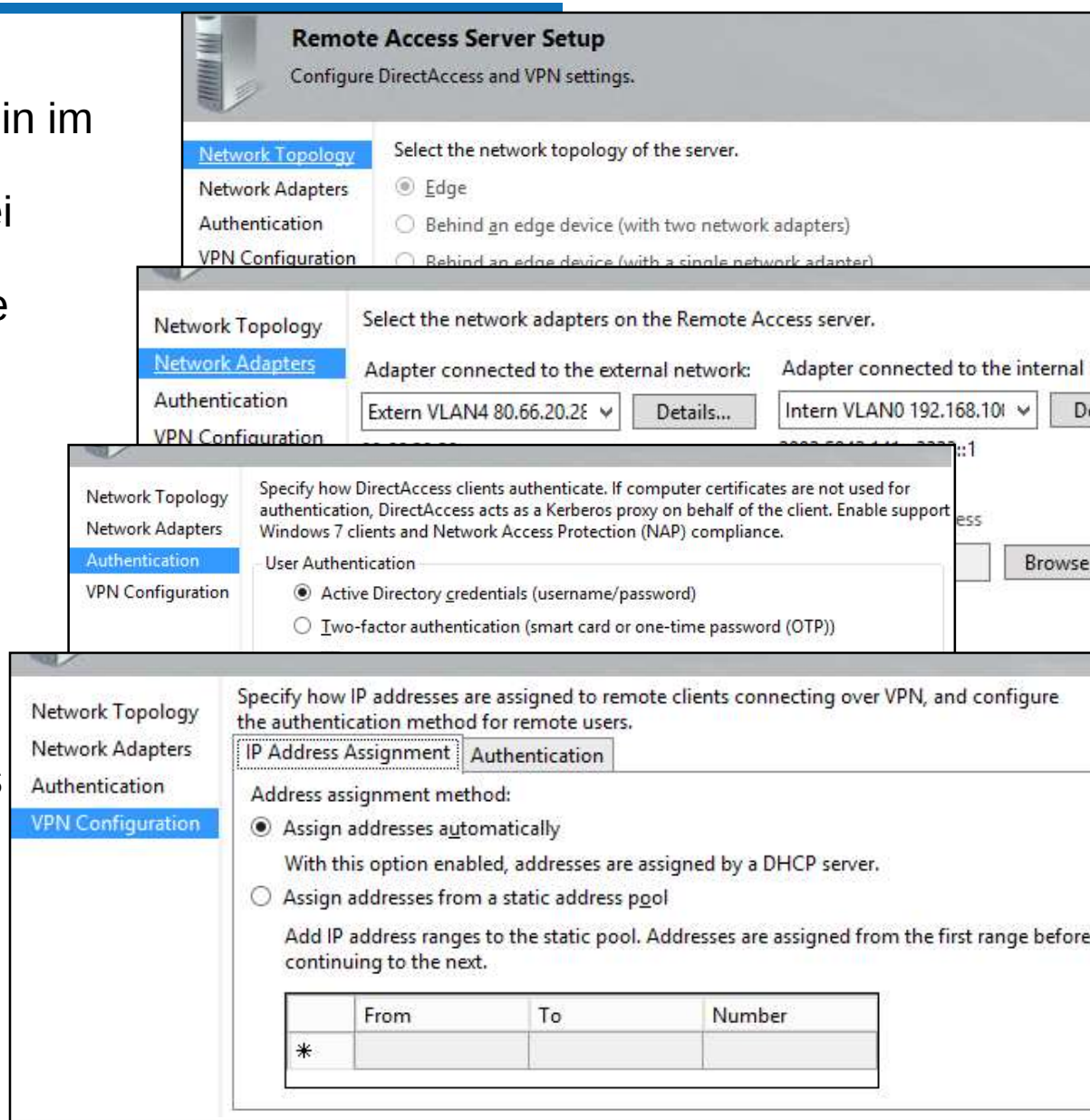




Schritt 2: Konfiguration des DA-Server

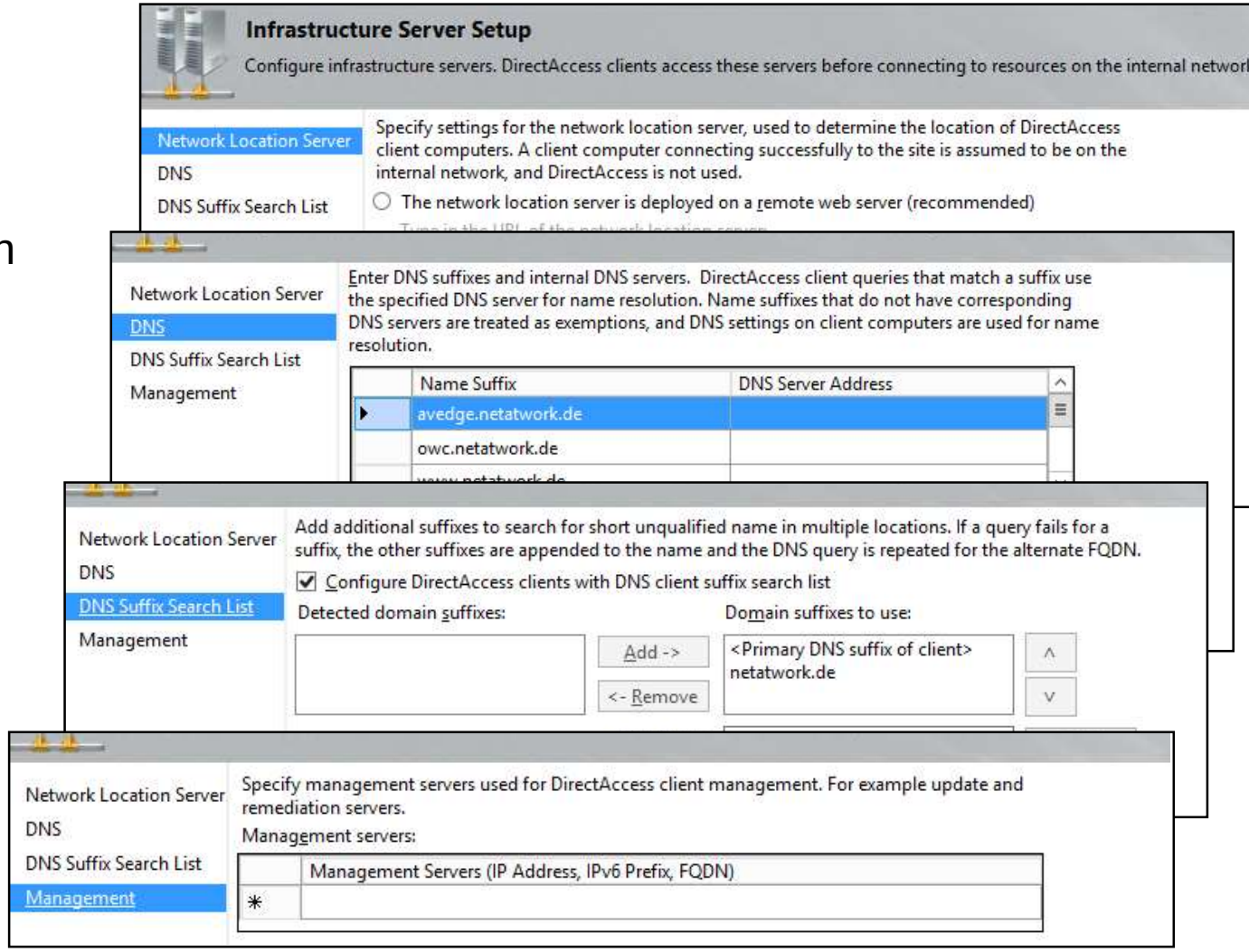
Net at Work
Building IT-Excellence.

- Topologie
  - Ohne Firewall d.h. ein Bein im Internet, eines intern
  - Hinter einer Firewall (zwei Netzwerkkarten)
  - Hinter einer Firewall (eine Netzwerkkarte)
- Konfiguration der Netzwerkkarten
  - IP-Adressen
  - Zertifikat
- Authentifizierung
  - AD oder MultiFaktor
  - Optional Zertifikate (erforderlich mit Windows Clients)
  - Optional NAP
- VPN Konfiguration



Step 3: Infrastruktur Server

- Network Location Server
  - Wie der Client erkennt, dass er extern oder intern ist
- DNS
  - Alternative DNS-Server und Ausnahmen pflegen
- DNS Suffix
  - Suchreihenfolge
- Management Servers
  - SCOM u.a.



Typische „Ausnahmen“

Net at Work
Building IT-Excellence.

- CRL Verteilpunkte
- IPHTTP-Server
- VPN-Server
- Lync Edge Server
- Extern per HTTP erreichbare Systeme
  - Exchange OWA
  - SharePoint
  - RDP-Gateway
  - UAG Portal
  - Office 365 Dienste
  - ADFS-Server

Step 4: Interne Application Server

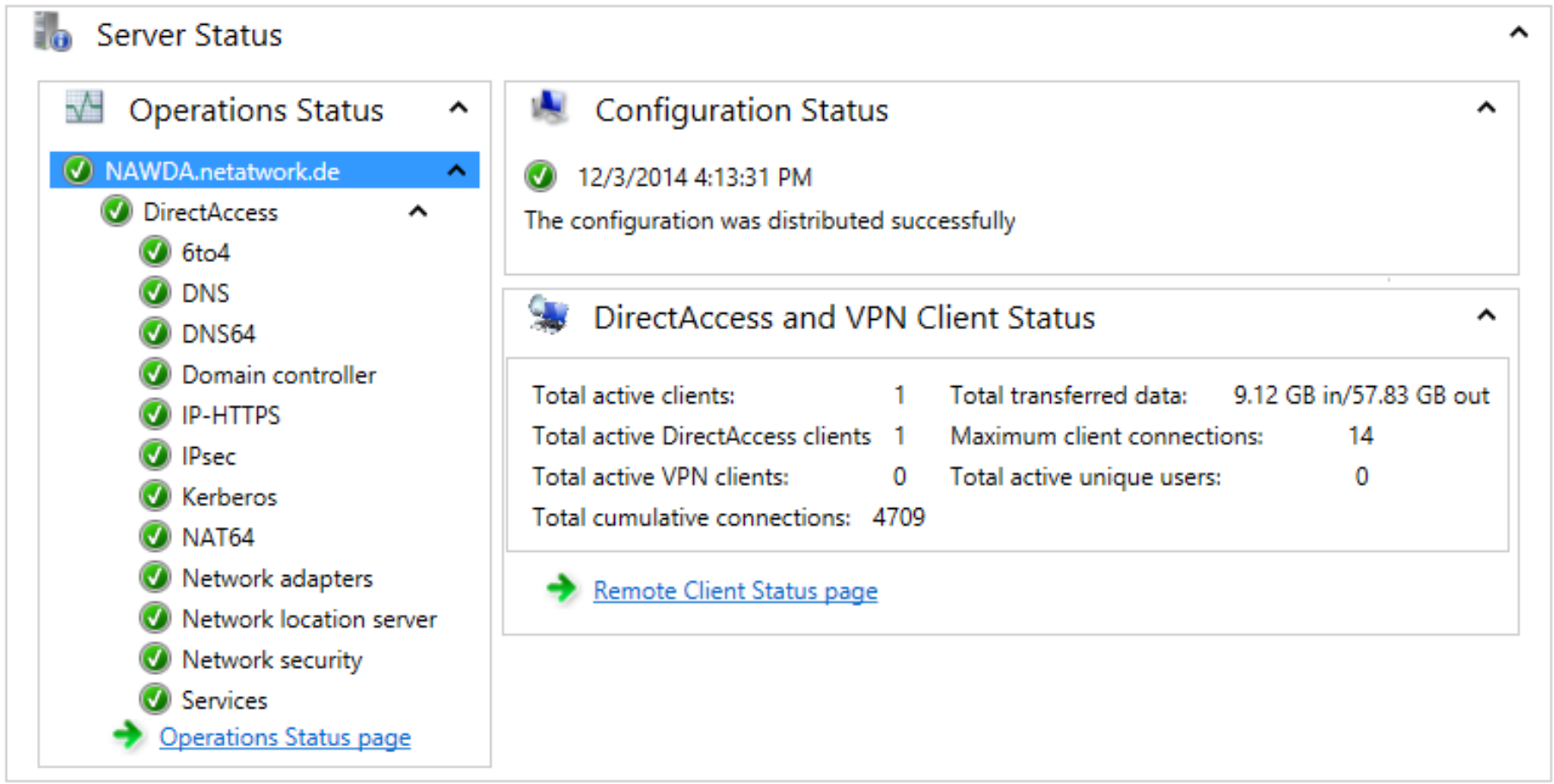
Net at Work
Building IT-Excellence.

Betrieb

Client, Server, Dienste, Counter

Management Client Dashboard

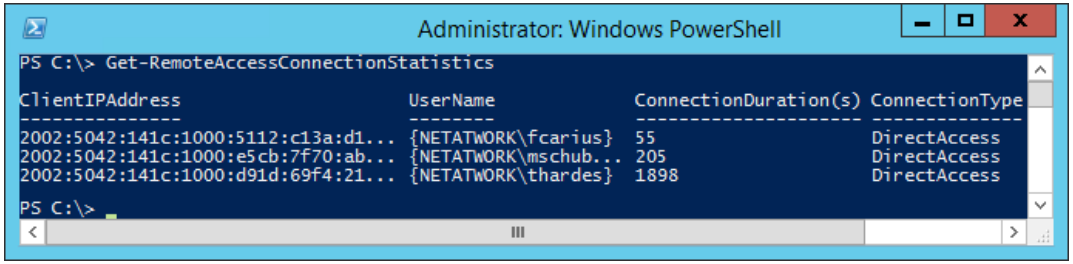
Net at Work
Building IT-Excellence.



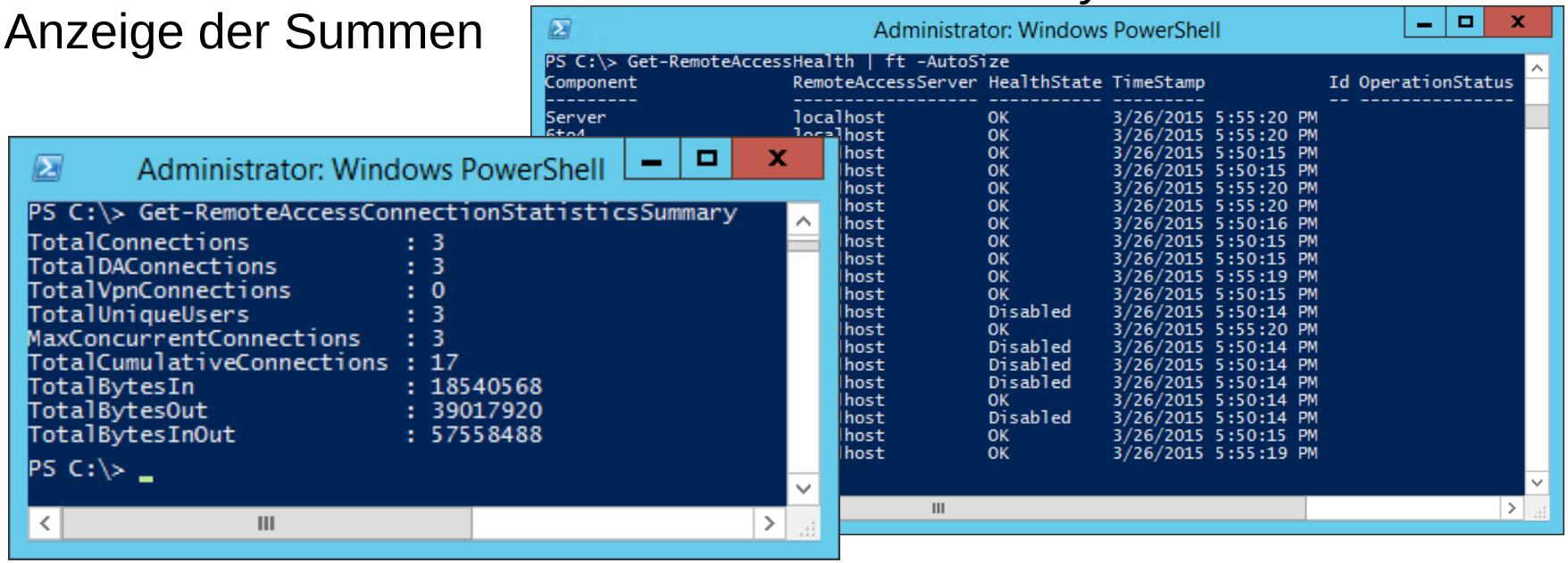
PowerShell auf dem Server

Net at Work
Building IT-Excellence.

- Get-RemoteAccessConnectionStatistics
  Anzeige der aktuell verbundenen Clients



- Get-RemoteAccessHealth
- Get-RemoteAccessConnectionStatisticsSummary
  Anzeige der Summen

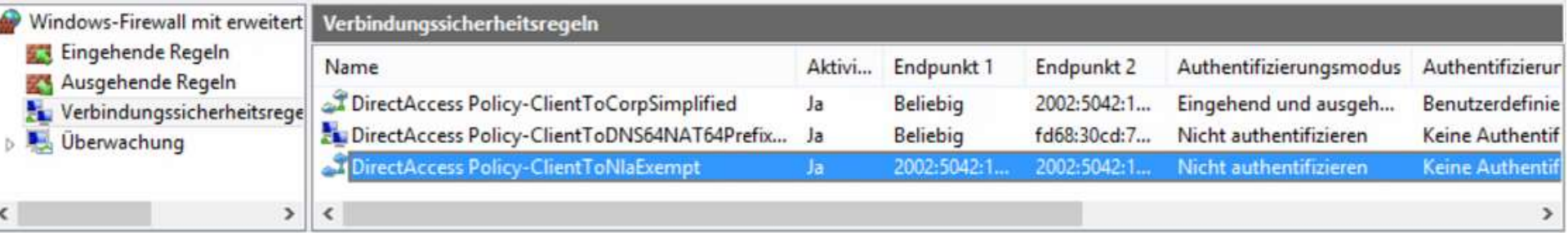


Fehlersuche auf dem Client

Net at Work
Building IT-Excellence.

- netsh namespace show policy
- netsh inter httpstunnel show statistic
- netsh inter httpstunnel show interface

```
PS C:\Users\adm-fcarius> netsh int httpstunnel show stat

Interface IPHTTPSInterface Parameters
------------------------------------------------------------
Total bytes received       : 1260537242
Total bytes sent           : 2903803810

Most Recent Client Address                Total Bytes In    Total Bytes Out
----------------------------------------- ----------------- -----------------

PS C:\Users\adm-fcarius> netsh int httpstunnel show int

Interface IPHTTPSInterface Parameters
------------------------------------------------------------
Role                       : server
URL                        : https://da.netatwork.de:443/IPHTTPS
Client authentication mode : none
Last Error Code            : 0x0
Interface Status           : IPHTTPS interface active
```



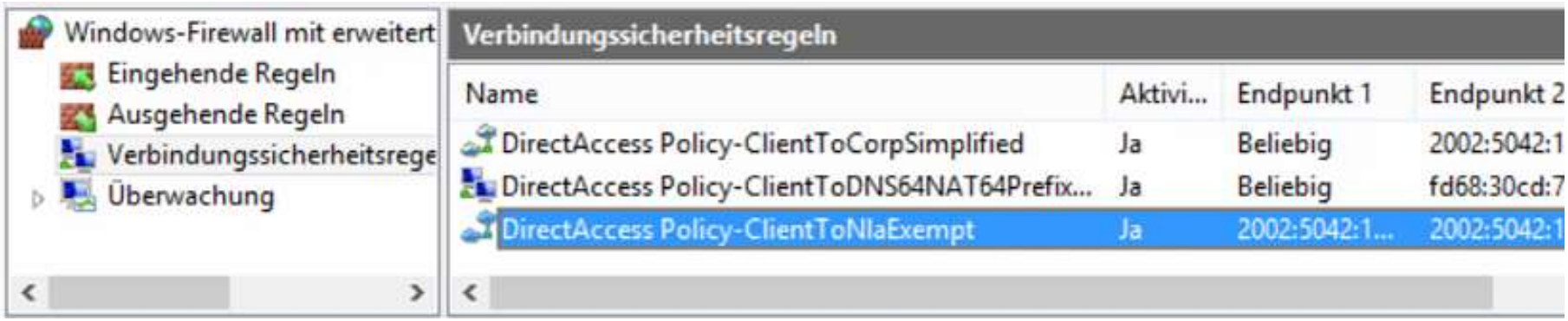
Fehlersuche auf dem Client

Net at Work
Building IT-Excellence.

- IPConfig /ALL

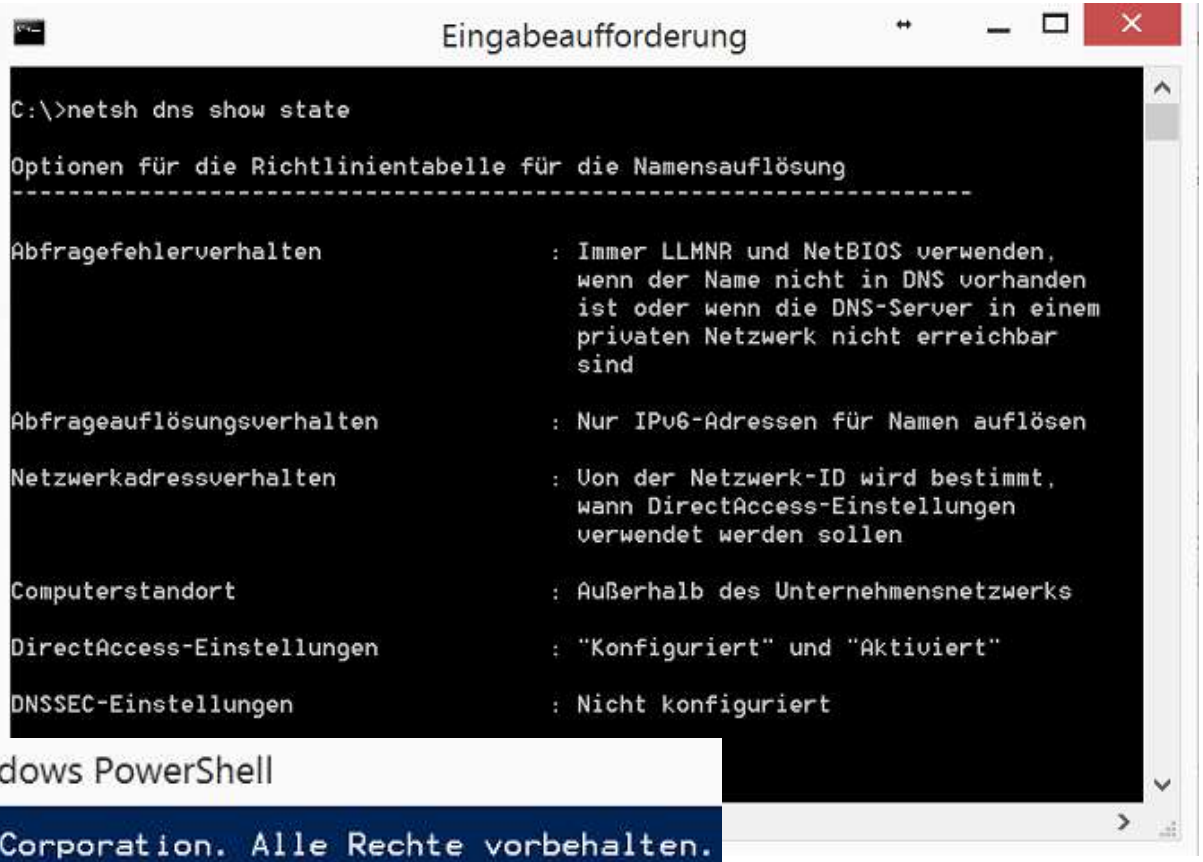
```
Tunneladapter iphttpsinterface:
   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . : iphttpsinterface
   Physische Adresse . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . : Ja
   IPv6-Adresse. . . . . . . . . . . : 2002:5042:141c:1000:a101:b18b:af84:c46a(Bevorzugt)
   Temporäre IPv6-Adresse. . . . . . : 2002:5042:141c:1000:5112:c13a:d1b:9647(Bevorzugt)
   Verbindungslokale IPv6-Adresse  . : fe80::a101:b18b:af84:c46a%19(Bevorzugt)
   Standardgateway . . . . . . . . . :
   DHCPv6-IAID . . . . . . . . . . . : 603979776
   DHCPv6-Client-DUID. . . . . . . . : 00-01-00-01-1C-66-64-11-F8-16-54-0A-00-F0
   NetBIOS über TCP/IP . . . . . . . : Deaktiviert
```

- Windows Firewall



Net at Work
Building IT-Excellence.

- netsh dns show state



- get-NetIPHttpsState

Kurz vorm Ziel

Vom Client zum Service

LAN, WAN, Internet, MPLS, VPN

Direct Access ist…

Net at Work
Building IT-Excellence.

- … eine faszinierende Technologie
- … einfach und schnell installiert
- … Bestandteil von Windows
- ... „konfigurationsfrei“ auf dem Client
- … konfigurationsarm auf dem Server
- … IPv6 sollte Sie nicht abschrecken.

- Einschränkungen bleiben
  - IPv4-Only Hosts sind nur über „Namen“ erreichbar
  - Clientsoftware muss IPv6 unterstützen
  - Windows Enterprise Version als Desktop

Fragen?

Kontakt:
Frank Carius, frank.carius@netatwork.de
Net at Work GmbH, Am Hoppenhof 32 A, Paderborn
+49 (5251) 304 600